POLICY 1305.00 Enterprise Information Technology
Issued April 12, 2007

SUBJECT: Policy for Enterprise Information Technology

APPLICATION: This policy is intended for statewide compliance and applies to all Executive Branch Departments, Agencies, Trusted Partners, Boards or Commissions using State of Michigan information networks and IT resources.

PURPOSE: To establish statewide Information Technology Policies, Standards and Procedures (PSP) that expands technological efficiencies through the use of common technology across the executive branch of State government. This policy further establishes the authority, responsibility and oversight for ensuring enterprise policies, standards and procedures are developed, implemented and enforced to protect the confidentiality, integrity and availability of State of Michigan (SOM) information.

CONTACT AGENCY: Michigan Department of Information Technology (MDIT)
Office of Enterprise Security

TELEPHONE: 517/241-4090

FAX: 517/241-2013

SUMMARY: Executive Order 2001-3 Creation of Department of Information Technology charged the Director of MDIT with the goal of achieving the use of common technology across the executive branch.

Duties include:

- Coordinating a unified executive branch strategic information technology plan.
- Developing and implementing processes to replicate information technology best practices.
- Overseeing the expanded use of project management principals.
- Serving as a general contractor between the State's information technology users and private sector providers of information technology.
- Developing service-level agreements with executive branch departments.
- Developing standards for application development including a standard methodology and cost benefit analysis.
- Determination of data ownership assignments among executive branch departments and agencies.
- Developing systems and methodologies to review, evaluate, and prioritize existing information technology projects.

Pursuant to Section 3(b) of the Executive Organization Act of 1965 (1965 PA 380) all of the transferred entities statutory authority, powers, duties and functions, records personnel, property, unexpended balances of appropriations, allocations or other funds, including the functions of budgeting and procurement, transferred to the receiving principal department.

The Executive Order defines information technology services as:

- Application development and maintenance.
- Desktop computer support and management.

- Mainframe computer support and management.
- Server support and management.
- Local area network support and management.
- Information technology contract, project and procurement management.
- Information technology planning and budget management.
- Telecommunication services, security, infrastructure and support.

Pursuant to Executive Order 2001-3, all information technology services currently within any executive branch department or agency and all authority, powers, duties, functions and responsibilities of following that are transferred from the Department of Management and Budget to the Department of Information Technology.

- the Michigan Administration Information Network.
- the Computing Services Unit.
- the Information Technology Services Division.
- the Office of Project Management.
- the Information Technology Budget and Finance Division.
- the Office of Information Technology Solutions.
- the Telecommunications Services Unit.
- the Michigan Information Network Office.
- the Michigan Information Center.

In an effort to meet the goals of achieving the use of common technology across the executive branch, while protecting the SOM information, a series of statewide Information Technology policies, standards and procedures will be developed.

Central to this approach is the adoption of Control Objectives for Information and related Technology (CoBIT) concepts, the guidance and principles from ISO 177999, and National Institute of Standards (NIST) Security best practices. The goal is for these objectives and best practices is to have agency internal policies, standards and procedures that complement the Enterprise Information Technology policies, standards and procedures and provide agencies the ability to protect the State's technology resources to the fullest extent possible. This enterprise approach to information security allows the State and its agencies to do so in a highly coordinated and efficient manner.

Organizational and technological changes make it necessary to redefine and communicate existing policies and develop new policies in order to maintain cohesive operations and uniform standards across the enterprise. To facilitate communication of policies across the enterprise, all the Enterprise Information

Technology policy and sub-policies will be placed in the DMB Administrative Guide; they will include, but not be limited to, the following type of sub-policies.

- Security Awareness Policy
- Information Security Policy
- Access Control Policy
- Network & Infrastructure Policy
- Application Security Policy
- Tools Policy
- Configuration Management Policy
- System and Services Acquisition Policy
- Continuity of Business Planning Policy

- POLICY:

Protecting citizen information is a priority for Michigan and its 19 agencies. The enterprise information security approach is a cross-agency solution geared toward establishing a statewide framework for information security and the basis for establishing a common technology across the executive branch of State government.

Through this approach, enterprise policies, standards and procedures will be developed by the State for agency use to empower a process with the direction and consistency necessary for successful process improvement. With these guiding principles in-hand, agencies are guided to map out the appropriate security controls in cooperation with MDIT to protect its assets. The results shall define the overall security direction for state employees and business partners.

- Agency responsibility as Data Owners:

  - Each Agency Director within their area of responsibility shall ensure:

    a. Management, technical and operational controls are in place that protect the reputation of the State and allows the State to satisfy its legal and ethical responsibility to protect the confidentiality, integrity and availability of the State’s information.
    b. All employees are aware of MDIT and agency internal policies, standards and procedures to carry out these policies. They also need to understand the legal constraints within which they are to function.
    c. Employees are advised of the necessity of complying with MDIT policies, and laws pertaining to the protection of State of Michigan Information because non-compliance may leave the State liable and employees vulnerable to prosecution and civil suit.
    d. Internal agency security polices and procedures are implemented, maintained and enforced that compliment and comply with this policy.
    e. Agencies desiring to implement more stringent policies than those developed by MDIT may do so in conjunction with MDIT.

- Agency responsibility as Data Custodian:

  - The Department of Information Technology Director shall ensure:

    a. A mechanism is in place to assist the agencies with implementing the appropriate security controls to protect the agency’s assets.
    b. A mechanism is in place that facilitates a statewide approach to information security.
    c. A mechanism is in place that helps to identify and prevent the compromise and misuse of the State’s information, applications, networks and computers.

d. A mechanism is in place to oversee and expand the use of project management principles.
e. Enterprise IT policies, standards and procedures necessary to facilitate the use of common technology across the executive branch of State government are developed and implemented.
f. All agencies have access to the Enterprise Information Technology policies, standards and procedures.
g. A mechanism is in place to provide an enterprise approach for creation and maintenance of secure systems across the SOM network and infrastructure.
h. A mechanism is in place to expand technological efficiencies related to common application development, customer support, desktop/laptop platforms, server consolidation, enterprise architecture solutions, risk assessments, shared data and greater citizen access, and expansion of network speed and capacity at lower cost.
i. A mechanism is in place to facilitate a development and implementation process to replicate information technology best practices.
j. A mechanism is in place to develop service-level agreements with Agencies.
k. A mechanism is in place to monitor and evaluate new and emerging technology, which maybe applicable for enterprise use, and determine the most effective way to introduce such technology into the current environment.
l. A mechanism is in place to develop systems and methodologies to review, evaluate, and prioritize existing and future information technology projects.
m. A mechanism is in place to acquire end user computing resources and services.

Terms and Definitions:

Agencies

Is the principal department of state government as created by Executive Organization Act 380 of 1965.

Availability

Ensuring timely and reliable access to and use of information and assuring that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

Confidentiality

Protecting information from unauthorized disclosure or interception and assuring that information is shared only among authorized persons and organizations.

Data Custodian

The individual or organization that has responsibility delegated by the data owner for maintenance and technological management of their data and systems.

Data/Information

Is SOM Agency information. No distinctions between the words data and information are made for purposes of this policy.

Data Owner

The person(s) with statutory or operational responsibility for the integrity, confidentiality, and availability of SOM data for their agency and for establishing the controls for generation, collection, processing, dissemination, and disposal of their agency data.

Information Technology Resources

Computers, storage peripherals, network equipment and wiring, network-attached printers and fax machines.

Integrity

Guarding against improper information modification and/or destruction, ensuring information has not been altered by unauthorized people and the assurance that the information can be relied upon to be sufficiently accurate for its purpose.

Technical Policy(ies)

High level executive management statements used to set directions in an organization that documents information values, protection responsibilities and management commitment for protecting its computing and information assets. Policies are strategic in nature.

Technical Standards

Published documents that contain technical specifications or other precise criteria designed to be used consistently as a rule, guideline, or definition. They are also a collage of best practices and business case specific to address the SOM's technological needs. Standards are tactical in nature and derive their authority from a policy.

Technical Procedures

A series of prescribed steps followed in a definite order which ensure adherence to the standards and compliance as set forth in the Policy to which the Procedure applies. Procedures are operational in nature and derive their guidance from a standard and authority from a policy.

Trusted Partner

Is a person (i.e. vendor, contractor, 3rd party, etc.) or entity that has contracted with the State of Michigan to perform a certain service or provide a certain product in exchange for valuable consideration, monetary, or goods and services.

- **Authority**

  Executive Order No. 2001 – 3, Creation of the Department of Information Technology

  E.R.O. No. 2001-1, compiled at § 18.41 of the Michigan Compiled Laws (Management and Budget Act 431 of 1984: Section 18, and Executive Reorganization Order 2001-1 now contained in the Act Section 18.41 Paragraph H).

  This policy obtains it's authority from Executive Order No. 2001 – 3. The enterprise policies, standards and procedures developed under the "1305 Enterprise Information Technology" policy set forth the Departments position on a given subject. Information technology standards and procedures cannot override the authority of any information technology policy.

  The "1305 Enterprise Information Technology" policy is the mechanism used for establishing and enterprise approach to information security and serves as the overarching umbrella policy for protecting the SOM information and assets. This policy and its supporting sub-policies should be considered collectively rather than as separate or unrelated.

  Therefore, in order to ensure a consistent implementation of information security practices, the information technology policies developed in the DMB Administrative Guide under "1305 Enterprise Information Technology" require mandatory compliance by all state agencies. The enterprise standards and procedures developed from these policies obtain its authority from the enterprise policies and are therefore mandatory as well.

- **Enforcement**

  Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and/or criminal prosecution where the act constitutes a violation of law.

  Any SOM partner found to have violated this policy may be subject to action, up to and including criminal prosecution where the act constitutes a violation of law. A breach of contract and fiduciary liability may also apply.

- **Developing Policies, Standards and Procedures**

  A revision to a policy, standard and procedure may be necessary and the Director of MDIT shall be responsible for implementing a mechanism to determine when the need to write or revise a policy, standard or procedure is warranted.

  All SOM Information Technology policies, standards and procedures shall be reviewed for needed revisions every two (2) years and revisions implemented one year later.

- **Exceptions**

  An exception to this policy directive shall be signed by the requesting agency Director, authorized by the Department of Information Technology Office of Enterprise Security (OES) Director, and granted only by the MDIT Director. Complete details for submitting and obtaining an exception can be found in the standards and procedures for this policy.

- **Effective Date**

  This policy will be effective immediately upon release.

* * *